

CCC:CMM
F.#2018R01256

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ JUL 13 2018 ★

LONG ISLAND OFFICE

IN THE MATTER OF THE SEARCH OF
(1) ONE BLACK LG CELLULAR
TELEPHONE, WITH A CRACKED
SCREEN, BEARING MODEL #: LG-
VS425LPP, S/N: 801VTTD2226505,
FCC ID: ZNFVS425PP, IMEI:
355156092235218 ("DEVICE 1");
(2) ONE DARK REFLECTIVE-COLORED
APPLE IPHONE CELLULAR
TELEPHONE, BEARING T-MOBILE SIM
CARD #8901260203 794142360, IMEI:
353046093883460 ("DEVICE 2");
ALL OF WHICH ARE CURRENTLY
LOCATED IN THE EASTERN DISTRICT
OF NEW YORK

APPLICATION FOR A SEARCH
WARRANT FOR ELECTRONIC
DEVICES

Case No. _____

MJ 18- 645

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Francis X. Rau, being first duly sworn, hereby depose and state as follows:¹

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—

¹ Because the purpose of this affidavit is to set forth only those facts necessary to establish probable cause for a search warrant, I have not described all the relevant facts and circumstances of which I am aware.

two electronic devices—which devices are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent with the Drug Enforcement Administration (“DEA”) for over 18 years. I am currently assigned to both the Long Island Heroin Task Force and the DEA Heroin Task Force. I have been involved in the investigation of numerous cases involving the trafficking of narcotics and the use of firearms in furtherance of narcotics trafficking. In the course of those investigations, I have conducted physical surveillance, debriefed cooperating witnesses and confidential informants, and interviewed civilian witnesses. I have participated in investigations involving search warrants, including searches of electronic devices, and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to communicate with one another and to conceal their activities from detection by law enforcement authorities.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code Section 841 and Title 18, United States Code, Section 924(c) have been committed (the “Target Offenses”). There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as described in Attachment B.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is (1) one black LG cellular telephone, with a cracked screen, bearing Model #: LG-VS425LPP, S/N: 801VTDD2226505, FCC ID: ZNFVS425PP, IMEI: 355156092235218 (“DEVICE 1”); and (2) one dark reflective-colored Apple iPhone cellular telephone, bearing T-Mobile SIM Card #8901260203 794142360, IMEI: 353046093883460 (“DEVICE 2”) (together, the “DEVICES”). The DEVICES are currently located in the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On June 24, 2018, law enforcement officers from the Long Island Heroin Task Force, including myself, were in the vicinity of East Farmingdale as part of an investigation into possible narcotics trafficking. Law enforcement officers observed Larry Carpenter engage in what they believed, based on their training and experience, was a narcotics sale with John Doe, an individual whose identity is known to the DEA. Joe Doe was observed exiting a white Pontiac Grand Am and, at the same time, Carpenter was observed in the immediate vicinity seated in the passenger seat of a green Honda Accord (the “Honda”). John Doe was then observed approaching the passenger window of the Honda. Law enforcement officers observed an exchange between Carpenter and John Doe that appeared, based on their training and experience, to be the exchange of drugs for money.

8. Thereafter, law enforcement officers followed the Honda for a brief period of time and observed the vehicle stop after something came out of the passenger window. Law enforcement officers then observed Carpenter exit the passenger seat of the Honda and backtrack to receive something from the ground. At that time, law enforcement officers pulled up near the Honda, and Carpenter began to run away. Carpenter was then apprehended in short order.

9. Almost simultaneously, the female driver gave officers consent to search the Honda and a firearm was located on the left side of the passenger seat closer to the center console in plain view. The female driver later told law enforcement officers that the gun recovered from the Honda belonged to Carpenter. The DEVICES were also recovered from the floor of the front passenger seat, where Carpenter had been sitting.

10. Around the same time, other law enforcement officers followed John Doe, thereafter performing a stop of his vehicle and retrieved from John Doe a substance that field-tested positive for the presence of cocaine. When questioned, John Doe told the officers that he had just purchased the crack cocaine from an individual known to him as "Dot" who was in a green Honda or Sentra. John Doe advised that he set up the purchase of the crack cocaine from Dot via text and had purchased crack from "Dot" before. John Doe later viewed a photo-array of six men including Carpenter. John Doe selected Carpenter and one other, but could not positively identify which of the two had sold him the crack cocaine. Despite that John Doe was unable to positively identify Carpenter, John Doe provided

“Dot’s” cell number as (631) 260-4547, which is a cell phone number known by law enforcement to be associated with Carpenter.²

11. Following his arrest, Carpenter provided law enforcement agents with the cell phone number for DEVICE 2 as (347) 424-6884.³ Subscriber information for cell phone number (347) 424-6884 is: Larry Carpenter, 72 Pearsall Avenue, Freeport, NY 11720.

12. Based on the above, there is probable cause to believe that Carpenter, as well as others whose identities are unknown at this time, were involved in the distribution and possession with intent to distribute a controlled substance and possession of a firearm in furtherance of such drug trafficking crime. Further, there is probable cause to believe that information on the DEVICES will produce evidence probative of the crimes under investigation.

13. Based on my training and experience, I know that individuals who engage in drug trafficking commonly use mobile devices such as cellular telephones to communicate with co-conspirators through voice calls, text messages, emails, and other means. I further know that individuals who commit such drug trafficking crimes often use mobile devices to arrange and plan the execution of the crimes.

² Subscriber information for cell number (631) 260-4547 is: Update Info, 295_Parkshore_Dr, Folsom, CA 95630.

³ Carpenter provided law enforcement officers with this cell phone number and gave officers limited consent to search the phone in order to obtain the telephone number of Carpenter’s girlfriend. At that time Carpenter accessed the cell phone to obtain his girlfriend’s telephone number, he stated out loud his passcode for the cell phone.

14. The DEVICES are currently in the lawful possession of the DEA after being recovered from Carpenter incident to his lawful arrest.

15. The DEVICES are currently located in the Eastern District of New York. I know that the DEVICES have been stored in a manner in which there contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES first came into the possession of the DEA.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital

data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the DEVICES have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, PDAs, and GPS navigation devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as

direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

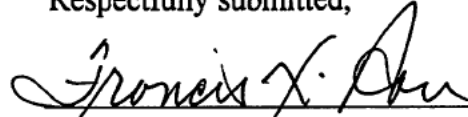
20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,


Francis X. Rau
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me
on July 13, 2018:


HONORABLE GARY R. BROWN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is (1) one black LG cellular telephone, with a cracked screen, bearing Model #: LG-VS425LPP, S/N: 801VTTD2226505, FCC ID: ZNFVS425PP, IMEI: 355156092235218 ("DEVICE 1"); and (2) one dark reflective-colored Apple iPhone cellular telephone, bearing T-Mobile SIM Card #8901260203 794142360, IMEI: 353046093883460 ("DEVICE 2") (together, the "DEVICES"). The DEVICES are currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICES described in Attachment A that relate to violations of Title 21, United States Code, Section 841 and Title 18, United States Code, Section 924(c) and involve Larry Carpenter and his co-conspirators, including:
 - a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;
 - b. lists of customers and related identifying information;
 - c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - e. any information recording Larry Carpenter's schedule or travel;
 - f. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of software that would allow others to control the DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the times the DEVICES were used;
5. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICES; and
6. Contextual information necessary to understand the evidence described in this Attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.